WHAT IS CLAIMED IS:

1. A system for managing volatile storage of information for operating a
device having extended periods of inactivity between periods of activity
comprising:
        volatile memory connected to receive said information from a
source and enabled to retain said information during power-on conditions;
        processing circuitry coupled to said volatile memory to process
said information during said periods of activity; and
        a volatile memory checker enabled to execute between said
periods of activity, said volatile memory checker including test code
configured to detect errors within said information retained in said volatile
memory.

2. The system of claim 1 wherein said volatile memory, said processing
circuitry and said volatile memory checker are integrated into a single
integrated circuit chip, said test code being configured to detect soft errors.

3. The system of claim 2 wherein said volatile memory is one or both of
dynamic random access memory (DRAM) and static random access memory
(SRAM) embedded within said integrated circuit chip, said processing circuitry
including a processing unit.

4. The system of claim 1 wherein said volatile memory checker includes a
timing module enabled to trigger execution of said test code in response to
detection of a passage of a preselected time period and simultaneous
detection that said device is in a period of inactivity.

5. The system of claim 1 further comprising a recovery module responsive
to said volatile memory checker to selectively trigger information replacement
for said volatile memory upon detecting said errors, said information being
executable code for operating said device.

1   6. The system of claim 5 wherein said recovery module is configured to
2   selectively reinitialize said device to initiate a transfer of said executable code
3   from said source to said volatile memory.

1   7. The system of claim 5 wherein said recovery module is configured to
2   selectively reset said device in response to a system-wide error in execution
3   of said executable code.

1   8. The system of claim 5 wherein said volatile memory checker is configured
2   to perform a cyclic redundancy check (CRC) or checksum of executable code
3   memory space of said volatile memory.

1   9. The system of claim 1 wherein said volatile memory, said processing
2   circuitry and said volatile memory checker are integrated into an application
3   specific integrated circuit (ASIC) of a printer controller.

1   10. The system of claim 1 wherein said volatile memory and said processing
2   circuitry are housed within separate integrated circuit chips.

1   11. A method of assessing integrity of executable code comprising the
2   steps of:
3   transferring said executable code into volatile memory of a
4   device that is activated upon execution of said executable code, said device
5   being in an inactive state between executions of said executable code;
6   performing time-based volatile memory checking routines in
7   response to detecting that said device is in said inactive state and a
8   preselected time period has elapsed, including checking code space of said
9   volatile memory to detect errors within said executable code; and
10   initiating a selected response upon detecting fatal code error
11   during performing said checking routines.

12. The method of claim 11 wherein said step of performing said routines includes calculating a cyclic redundancy check (CRC) or checksum for executable code space of said volatile memory.

13. The method of claim 11 wherein said step of initiating said selected response includes triggering a reinitialization that repeats said step of transferring said executable code into said volatile memory.

14. The method of claim 13 wherein said step of initiating further includes resetting said device in response to a code error that results in said checking routines being terminated.

15. The method of claim 11 wherein said step of transferring includes loading said executable code into random access memory embedded in an integrated circuit having a central processor.

16. The method of claim 15 wherein said step of performing said checking routines includes scheduling said checking routines to occur on a periodic basis.

17. An integrated circuit comprising:

a processor;

embedded volatile memory having an input to receive executable code that includes instructions specific to operations of said processor;

an integrated self-tester having stored test code specific to detecting code error in said executable code during storage in said volatile memory, said self-tester being responsive to a time-based test initialization signal for triggering periodic testing; and

a recovery module responsive to said self-tester to induce an operational sequence that transfers fresh executable code to said input of said volatile memory when said self-tester detects a specific code error condition.

1   18. The integrated circuit of claim 17 wherein said volatile memory is one or
2   both of dynamic random access memory (DRAM) and static random access
3   memory (SRAM), said specific code error condition including alpha particle-
4   induced error detections that are pre-identified as being fault conditions.

1   19. The integrated circuit of claim 17 wherein said self-tester includes
2   embedded non-volatile memory for storing said test code.

1   20. The integrated circuit of claim 17 wherein said processor and said
2   executable code are specific to operating within a printer controller.

1   21. The integrated circuit of claim 17 wherein said recovery module includes
2   code for inducing reinitialization in which said volatile memory is reloaded with
3   said executable code from a source of said executable code.

1   22. A system for managing information storage comprising the steps of:
2   storing said information within memory that is susceptible to
3   occurrences of soft errors, said memory being within a device that is
4   characterized by extended periods of inactivity between periods of activity;
5   processing circuitry coupled to said memory to process said
6   information during said periods of activity; and
7   an automated memory checker enabled to execute between
8   said periods of activity, said automated memory checker being configured to
9   execute test code on a timed basis to detect said soft errors within said
10   information stored in said memory.

1   23. The system of claim 22 wherein storing said information in memory
2   includes magnetically recording said information on a medium susceptible to
3   said occurrences of soft errors.

1   24. The system of claim 22 wherein storing said information includes
2   embedding said information within non-volatile memory housed within an
3   integrated circuit chip, wherein said non-volatile memory is susceptible to said
4   occurrences of soft errors.